

Environmental Protection Agency Office of Environmental Information PROCEDURES for Disk Sanitization

Approval Date: 08/14/2006
Review Date: 08/14/2009

I. Subject: All electronic information and licensed software must be properly removed when disposing of computers with hard drives. A large volume of electronic information is stored on computer hard disk and other electronic media throughout the Environmental Protection Agency (EPA). Much of this information is sensitive to disclosure due to its confidentiality. Most of the software at EPA is licensed under special agreements which prohibit the transfer of this software outside of the Agency. This applies to all other electronic storage media including, Personal Digital Assistance (PDAs), removable media such as CDs, DVDs, Universal Serial Bus (USB drives), Zip drive media, Jaz drives, backup disks, diskettes and tapes.

II. Purpose: Unauthorized disclosure of certain information could subject the Agency to legal liability, negative publicity, monetary penalties, and the possible loss of funding. This procedure is designed to ensure that IT resources do not contain information of a confidential nature before they are transferred outside of any US Environmental Protection Agency facility or Region, for surplus or destruction. IT resources and electronic storage media will be cleaned of all information. Anything categorized as National Security Information Systems is not covered by this procedure.

III. Procedures: EPA staff and EPA contractors must use approved techniques for proper sanitization (See Definitions) of hard drives and electronic storage media. EPA staff and EPA contractors must ensure that any Agency records stored on computer hard disks or electronic media are properly identified and captured in the Agency's recordkeeping system in accordance with Agency policy and procedures prior to disk sanitization. Techniques include:

1. Ensure that all Agency records are properly identified and captured:
 - Until full deployment of the Enterprise Content Management System (ECMS), the Agency's approved recordkeeping system is paper-based and the current policy for capturing and maintaining any electronic records is "print and file".
 - These records must be maintained for the duration of their approved retention period. (See Records Schedule available on-line, <http://intranet.epa.gov/records/schedule/index.htm>).
 - In some cases, printing may cause loss of context, (e.g., databases and complicated spreadsheets). In those cases, the records may be maintained electronically, but must be readable, accessible and usable for the entire life of the records and dispositioned in accordance with the applicable records schedule.
2. Overwriting hard drives utilizing Department of Defense (DOD) accepted software. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information, effectively rendering the data unrecoverable. As a minimum, a triple pass overwrite method should be used, where data is overwritten with 0's, then 1's, and then once with pseudo random data. Any system containing a hard drive or electronic storage media that has information categorized as high confidentiality it must be overwritten seven times with a pattern of 0's, then 1's, and so on. A random test of hard drives should be made after overwriting. **Note:** After overwriting, the hard drive is still physically functional and can accept formatting. Therefore the PC can be reissued and used within the Agency.
3. Degauss (See Definitions) a hard drive or storage media to randomize the magnetic domains – most likely rendering the drive or media unusable in the process. If they cannot be economically repaired or sanitized for reuse by the available tools, then the media will be degaussed and discarded via the Recycling Electronics and Asset Disposition (READ) service (See Definitions). This option followed by physical destruction, must be used for any system containing a hard drive or electronic storage media that has information categorized as high confidentiality. If degaussing is performed "in house" at EPA, then a random test of hard drives should be made after degaussing. Properly applied, degaussing renders any previously stored data on magnetic media unreadable by keyboard or laboratory attack.

4. Physically destroying the storage media, rendering it unusable. Hard drives should be destroyed when protection can not be reliably ensured or the technology is old or can not be handled by the available tools. If they can not be economically repaired or sanitized for reuse, the media will be destroyed and discarded via the READ service. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive or storage media.
5. For destruction of a CD/DVD, the most economical form of destruction is a CD/DVD shredder.
6. Zip drive media, flash/USB drives should be physically destroyed.

IV. Sanitization

Tools: See Attachment 1.

V. Audience: All Program Offices, Regional sites and Laboratories of the EPA are subject to this guidance.

VI. Background: Studies of disk sanitization indicate that simply deleting files from the media or formatting a hard drive is not sufficient to completely erase data so that it cannot be recovered. Also, when you delete files in Windows by moving them into the Recycle Bin all data remains on the hard disk. These studies generally recommend two methods for disk sanitation. First method is the destruction of the media either by physical force or by electromagnetic degaussing. However, destroying a hard drive lessens the value of the computer system for any other use. The second method is disk sanitization, the overwriting of all previously stored data with a predetermined pattern of meaningless information, such as a binary pattern, its complement, and an additional third pattern. This has been detailed in the US Department of Defense National Industrial Security Program Operating Manual DoD 5220.22-M (see <http://www.dss.mil/isec/chapter8.htm>).

VII. Authorities:

- EPA Order # 2195.1 A4, Agency Network Security Policy, sub order # 2.3.5.

- Federal Information Processing Standards (FIPS 200), Minimum Security Requirements for Federal Information and Information Systems
<http://csrc.nist.gov/publications/fips/index.html>
- EPA Order #2161, Agency Records Management Policy, April 2006.

VIII. Waivers: Waivers for these Procedures will not be considered.

IX. Roles and Responsibilities:

The primary responsibility for sanitizing computer systems, electronic devices and media, rests with the Program Offices, Regions or the local Custodial Office. Additional responsible parties:

1. Information Management Officials (IMOs) or their designees are responsible for the sanitization of all EPA-owned electronic devices and computer systems in their Program Offices or Regions prior to removal from any EPA facility. This responsibility may be delegated within the Program Office or Regions as deemed appropriate.
2. All EPA employees and EPA contractors are responsible for the sanitization of computer systems and other electronic storage media as described by these procedures before disposal.

X. Definitions: *Degauss* – to neutralize (erase) the magnetic field. Degaussing a magnetic storage medium removes all the data stored on it. An electromagnetic degausser is a device used for this purpose.

Sanitization, sanitized – is the end result after all data is obliterated. This includes all associated file system structures, operating system formatting and information from fixed disk or electronic storage media.

Recycling Electronics and Asset Disposition (READ) service – is an EPA managed Government Wide Acquisition Contract (GWAC) that provides Federal agencies with a dependable method of properly managing electronic inventories, recycling electronic equipment, and disposing of excess or obsolete electronic equipment in an environmentally responsible manner.
<http://www.epa.gov/oam/read/>.

XI. Recertification

Date: Three years from approval date.

**XII. Additional
Information**

Please contact Enterprise Desktop Solutions Division at 202 566-1800.

Attachment 1

(The suggested tools referenced below are current as of 1/6/06)

These are the tools used for overwriting hard drives using DOD approved packages:

- WipeDrive 3.0 www.whitecanyon.com
 - Windows Platform – DOD approved. Erases files, folders, cookies, or an entire drive.
- CyberScrub www.cyberscrub.com
 - Windows Platform – DOD approved. Erases files, folders, cookies, or an entire drive. Implements Gutmann patterns.
- DataScrubber www.scsitoolbox.com/products/DataScrubber.asp
 - Windows, Unix Platforms – DOD Approved. Handles SCSI remapping and swap area. Claims to be developed in collaboration with the US Air Force Information Welfare Center.

EPA recommends but does not endorse the following products:

Tools for degaussing hard drives:

- HD-1 All Media Degausser
The HD-1 erases virtually all formats of tape, diskettes and hard-disks up to 160 GB. Please note; hard drives are not reusable once degaussed.
- Model 8000 Hard Drive/Media Degausser
The Model 8000 Table Top unit is a low noise, compact unit with “industrial strength” flux fields and features a foot-control for hands-free operation.

Tools used for CD/DVD shredding:

- PRIMERA Disc Shredder – DS360
- Alera Technologies DVD/CD Shredder Plus XC
- Kobra 240 SS4
- HSM Model 125.2 Shredder
- Intimus 502CD CD Shredder
- Olympia 1500 CD Shredder